

VŠB-TECHNICKÁ UNIVERZITA OSTRAVA

Hornicko-geologická fakulta

Institut ekonomiky a systému řízení

BAKALÁŘSKÁ PRÁCE

Ostrava 2010

Miroslav Jančík

VŠB-TECHNICKÁ UNIVERZITA OSTRAVA

Hornicko-geologická fakulta
Institut ekonomiky a systémů řízení

Prostředky pro realizaci Internetu věcí
HW and SW for Internet of Things

Vedoucí bakalářské práce:

doc. Dr. Ing. Oldřich Kodym

Datum zadání: 31.10.2009

Datum odevzdání: 30.4.2010

Ostrava 2010

Miroslav Jančík

Prohlašuji:

- Byl jsem seznámen/a s tím, že na moji závěrečnou práci se plně vztahuje zákonč.121/2000 Sb. – autorský zákon, zejména § 35 – využití díla v rámci občanských a náboženských obřadů, v rámci školních představení a využití školního díla a § 60 –školní dílo.
- Beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo závěrečnou práci nevýdělečně užít ke své vnitřní potřebě(§ 35 odst.3).
- Souhlasím s tím, že jeden výtisk závěrečné práce bude uložen v Ústřední knihovně VŠB-TUO k prezenčnímu nahlédnutí a jeden výtisk bude uložen u vedoucího závěrečné práce. Souhlasím s tím, že údaje o závěrečné práci, obsažené v abstraktu, budou zveřejněny v informačním systému VŠB-TUO.
- Bylo sjednáno, že užít své dílo – závěrečnou práci nebo poskytnout licenci k jejímu využití, mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).
- Závěrečnou práci anebo dílem se myslí bakalářská práce v případě bakalářského studia, diplomová práce v případě magisterského studia a disertační práce v případě doktorského studia.

Prohlašuji, že jsem celou bakalářskou práci včetně příloh vypracoval samostatně a uvedl jsem všechny použité podklady a literaturu.

V Ostravě

.....
Plné jméno studenta

Adresa trvalého pobytu studenta
Miroslav Jančík
Karla pokorného 1355/61
Ostrava 708 00

ABSTRAKT

Tato bakalářská práce je zaměřena na internet věcí a na prostředky pro realizaci internetu věcí. Práce informuje o dnes dostupných prostředcích pro realizaci internetu věcí jako je například RFID technologie. Zabývá se, jak internet věcí vypadá dnes a jak bude vypadat v budoucnosti. Práce představuje internet věcí jako distribuovaný a izolovaný informační systém. Práce poukazuje na výhody, nevýhody a nebezpečí internetu věcí dnes a v budoucnosti.

ABSTRACT OF THESIS

This thesis is aimed at "internet of things" and resources for its realization. In the first part technologies available today are discussed, such as RFID followed by description of present "internet of things" situation and estimation of future development of this technology. Second part analyse "internet of things" as an isolated and distributed IT system and describes advantages and disadvantages if this technology today and in future.

KLÍČOVÁ SLOVA

Internet věcí, Internet věcí jako distribuovaný informační systém, internet věcí jako izolovaný informační systém, RFID technologie, tag, EPC, senzory, funkce internetu věcí.

KEYWORDS

Internet of things, Internet of things as distributed information system, internet of things as isolated information system, RFID technology, tag, EPC, sensors, function on internet of things. Abstrakt

Obsah

1	Úvod	1
2	Internet věcí	1
2.1	Jak vzniká internet věcí	2
2.2	Prostředky pro tvorbu IoT	2
2.2.1	Hardware IoT	2
2.2.2	Software IoT	3
2.2.3	Další prostředky	4
2.3	RFID	4
2.3.1	Jak FUNGUJE RFID	4
2.3.2	EPC	4
2.3.3	Rozdělení RFID	5
2.3.4	Využití RFID	6
2.3.5	řešení pomocí RFID	7
2.3.6	Nebezpečí RFID	11
2.4	Překážky IoT	12
2.5	IoT dnes	16
2.5.1	Pachube.com	16
2.5.2	IBM řešení pomocí senzorů	17
2.5.3	Arduino	18
2.5.4	Fedex senseaware	19
2.5.5	Violet	19
2.5.6	WideNoise	21
2.6	Budoucnost IoT	21
3	IoT jako distribuovaný informační systém	22
3.1	Co je distribuovaný IS	22
3.2	Struktura distribuovaného IS	23
3.3	Výhody distribuovaného IS	23
3.4	Řešení distribuovaného IS v IoT v budoucnu	23
3.4.1	Celosvětový IS	24
3.4.2	Pachube	24
3.4.3	Systém bezpečnosti provozu	24
3.5	Zhodnocení	25

4	IoT jako lokální (izolovaný) informační systém.....	25
4.1	Struktura Izolovaného systému IS	26
4.2	Výhody izolovaného IS v IoT.....	26
4.3	Řešení izolovaných IS v IoT v budoucnu.....	26
4.3.1	Ovládací systém domu	26
4.4	Zhodnocení.....	28
5	Srovnání funkcí IoT	28
5.1	Kladné funkce IoT	29
5.1.1	Sledování produktů.....	29
5.1.2	Ovládání věcí přes internet	29
5.1.3	Informovanost	29
5.1.4	Bezpečnost světa	29
5.2	Rizika IoT	30
5.2.1	Ohrožení kritických procesů	30
5.2.2	Narušení soukromí.....	30
5.2.3	Nebezpečí terorismu.....	31
5.2.4	Humánní hledisko	31
6	Závěr.....	32
	Seznam použité literatury a zdrojů	34
	Seznam použitých symbolů a zkratek	35
	Seznam obrázků.....	36

1 Úvod

Během minulého století a desetiletí jsme mohli vidět velký rozmach Výpočetní techniky. Všechno na světě, naše planeta, přírodní systémy, lidské systémy, fyzikální objekty vždy vytvářeli veliké množství dat, ale tyto data jsme nemohli slyšet, vidět ani zachytit je. Nyní můžeme, protože máme na to přístroje a zařízení, které se dají dnes všechny mezi sebou propojit. Na světě je přes 6,5 miliardy lidí z toho se odhaduje, že dnes využívá internet asi 1,2 miliardy lidí. Podle tempa růstu se odhaduje, že během pár příštích let hodnota vzroste na 2 miliardy. A to je opravdu mnoho lidí a mnoho dat, které lidé vytvářejí. Ale data na internetu nevytvářejí jen lidé, ale jsou to přístroje, které jsou mezi sebou propojeny pomocí sítí. Jsou to například různé senzory (snímače teploty, dopravní senzory, (GPS). Nebude to trvat dlouho a bude více věcí na internetu, než jsou lidé na internetu. A to je právě Internet věcí. Internet věcí neznamena, že přes nějakou věc, třeba televizi budete ovládat internet, ale naopak přes internet budeme ovládat věci.

2 Internet věcí

Internet věcí teprve jako takový ještě vzniká, ale je to jen otázka času kdy začne fungovat tak, jak to známe ze sci-fi filmů. Některé služby, které určitě jsme každý z nás využili, aniž bychom tušili, jde o internet věcí. Například české dráhy na svých internetových stránkách zprovoznili službu „poloha vlaků“, zde zadáte číslo vlaku a vidíte, kde se vlak nachází a jestli má zpoždění. Vzhledem k rozmachu mobilních telefonů, které umožňují prohlížení webových stránek ve stejném rozsahu jako stolní počítače. Proto není problém kdykoliv a odkudkoliv se připojit k internetu. Mobilní signál ve vyspělých zemích dosahuje velmi velkého pokrytí. Proto se lze pomocí mobilu připojit skoro odkudkoliv. Navíc zde máme velký rozmach Wi-Fi sítí s připojením na internet zdarma. Dnes skoro každý má mobilní telefon, ten většinou patří jednomu danému člověku, a není problém vyhledat, kde se mobil právě nachází. Firma T-mobile už před 7 lety nabízela službu „kde je“, zde jste zadali telefonní číslo mobilu a přístupový kód a okamžitě Vám informační systém zobrazil lokalizaci mobilu na mapě. Tato služba spadá také pod internet věcí.

Tady se dostáváme, že k zavedení internetu věcí jsou nutné čidla, GPS a jiné senzory. Nutné jsou taky informační systémy zpracovávající data. Internet věcí se velmi rychle vyvíjí, protože přicházejí nové technologie. Nebude to zřejmě v blízké budoucnosti,

ale věřím, že jednou budeme moci přes internet ovládat skoro všechno, od brány domu až po světla či Hi-fi věže v obýváku.

2.1 Jak vzniká internet věcí

Internet věcí je teprve na začátku svého vývoje a vyvíjí se každým dnem, dnes už existuje mnoho izolovaných systémů, které využívají mnoho senzorů a zpracovávají a ukládají data do informačního systému. Tyto data slouží pouze pro „úzký“ okruh uživatelů. Vize internetu věcí je, že data budou zpřístupněna o všech předmětech a všem.

Některé firmy se snaží internet věcí zpřístupnit lidem už i do domácností. Příklady si uvedeme v bodě 2.5. IoT dnes.

2.2 Prostředky pro tvorbu IoT

2.2.1 Hardware IoT

Je to všechno zařízení, které se dá fyzicky osahat a souvisí s internetem věcí. Příklady si uvedeme dále.

2.2.1.1 Senzory

Jsou to zařízení, které kontrolují danou fyzikální veličinu a převádějí ji na signál, který je dále zpracováván. Senzory mohou sbírat data o čemkoliv, kde se dá měřit fyzikální veličina. Senzory teploty sbírají data o teplotě. Senzory sledování dopravní sítě na cestách. Senzory vlhkosti, mohou sledovat vlhkost vašeho trávníku a podle potřeby se automaticky spustí zavlažování. Senzory polohy mohou sledovat, polohu věci kdekoliv. Senzory jsou velmi důležitou součástí internetu věcí

2.2.1.2 RFID

Je to technologie Radiofrekvenční identifikace, tato technologie je také stále ve vývinu mnoho věcí usnadňuje. O RFID se zabývám v bodě 2.3.

2.2.1.3 GPS

Globální polohový systém, jde původně o vojenský systém, který s přesností desítek metrů určí polohu kdekoliv na Zemi. Dnes s použitím dalších metod výpočtů se přesnost udává na centimetry. Dnes GPS se využívá hojně v navigacích. A pomocí GPS se sledují například kontejnery určené pro námořní přepravu.

2.2.1.4 čtecí zařízení

Je to zařízení, které přijímá signál a data ze senzorů po té jdou ze čtecího zařízení do informačního systému

2.2.1.5 Počítačové sítě

Počítačová síť je propojení dvou a více počítačů, které sdílejí své prostředky. Mohou sdílet jak hardwarové tak softwarové prostředky. Počítačové sítě procházejí také stále inovacemi a tím se zvyšuje rychlost počítačových sítí. Počítačové sítě se rozdělují na LAN, MAN a WAN. Dnes si žádná firma nedokáže představit, že by fungovala bez počítačových sítí. Počítačové sítě umožňují rychlejší a dokonalejší komunikaci mezi pracovníky firmy. Počítačové sítě v internetu věcí mají hlavně funkci, že přenášejí data od snímačů do informačních systémů. Časem bude tato komunikace probíhat vzájemně. Že věci nebudou data o sobě jen posílat, ale budou je i přijímat a chovat se podle instrukcí.

2.2.2 Software IoT

Software je programové vybavení počítače v našem případě jsou to informační systémy, ovládací systémy a podpůrné systémy.

2.2.2.1 Ovládací systém

Dnes takovým příkladem mohou být SCADA systémy. Jsou to vizualizační systémy, které pomáhají řídit provoz, výrobu nebo nějaký proces. Tyto procesy jsou sice většinou řízeny z blízkosti od daného procesu, ale například Skupina ČEZ, ovládá přečerpávací nádrž Dlouhé Stráně na Moravě z řídicího velína v Čechách. V budoucnu budeme pomocí ovládacích systémů, ovládat a řídit věci kolem nás. Od nastavení ledničky po zapnutí myčky, pračky.

2.2.2.2 Informační systém

Informační systém slouží ke sběru, uchovávání, zpracování dat a k prezentaci dat. Je velmi důležitou součástí každé firmy. Informační systém se samozřejmě skládá z hardwaru, softwaru, orgwaru¹ a lidí, ale zde mám namysli, hlavně software. Budoucnost v informačních systémech vidím v tom, že dojde k propojení různých informačních systémů a přes jeden informační systém se dostaneme k datům čehokoliv na světě.

¹ Orgware- Jsou to organizační prostředky tvořené souborem nařízení a pravidel definujících provozování a využívání informačního systému.

2.2.3 Další prostředky

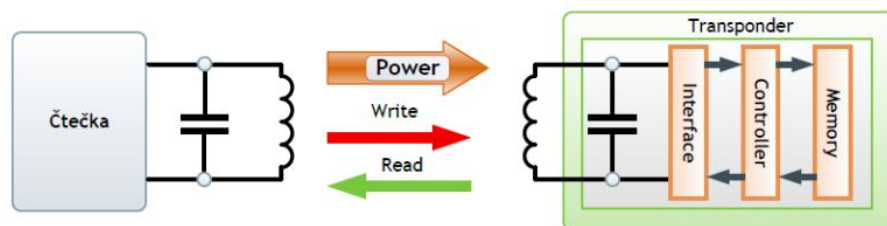
Samozřejmě Internet věcí netvoří jen hardware a software, ale jsou to hlavně lidé, kteří vyvíjejí, tvoří a internet věcí budou využívat nebo využívají. Tvorba internetu věcí se nesmí nechat vytvářet jen soukromým sektorem, je třeba dodržovat různé zákony. U nás v Evropě se o standardizaci a určování pravidel stará Evropská unie. Internet věcí přináší mnoho ulehčení každodenního života, ale bohužel přináší i nové problémy, které se musí řešit. Evropská unie dává do výzkumu internetu věcí mnoho peněz. O vytváření internetu věcí v Evropě se podílí také European Research Cluster on the Internet of Things – IERC, tento klastř byl vytvořen jako ambice Evropy pro vývoj Internetu věcí a RFID.

2.3 RFID

RFID je technologie velmi spjatá s internetem věcí. Slouží k jednoznačné identifikaci, sběru a uchovávání dat a lokalizaci jakéhokoliv předmětu, ke kterému je připevněn RFID čip. Díky klesáním cenám RFID je tato technologie na vzestupu a jednou nahradí čárové kódy.

2.3.1 Jak FUNGUJE RFID

Identifikační systém se skládá z transpondérů (tagy), čtečky a podpůrné systémy (řídící počítače, databáze, počítačové systémy). Čipy mohou být jak aktivní tak pasivní. U pasivních tagů využívají pro napájení energii vyslanou čtecím zařízením. Pomocí indukovaného napětí se nabije kondenzátor a čipy vysílají své informace. Informace vysílané čipem zachytí čtecí zařízení a data přenáší do informačního systému.



Obrázek 1 Princip funkce RFID

2.3.2 EPC

EPC je standardizovaný kód (Electronic Product Code), identifikuje jednoznačně nejen produkt, ale i položku produktu. Představme si čárový kód, který můžeme vidět na

každém výrobku v obchodě. V obchodech můžeme nejvíce vidět čárové kódy typu GTIN13.



Obrázek 2 GTIN13 čárový kód

První tři číslice označují zemi, další číslice identifikují výrobce a další identifikují produkt.

Standard EPC zahrnuje:

- Hlavičku – definuje typ údaje v EPC, jeho verzi
- EPC manager- identifikuje organizaci (vydavatele tagu)
- Objekt Manager – identifikuje druh produktu
- Sériové číslo produktu.

EPC = Electronic Product Code



Obrázek 3 Schéma EPC kódu

2.3.3 Rozdělení RFID

RFID čipy se dělí podle frekvenčního rozsahu:

LF – Používá frekvenci 125 kHz a 134 kHz, minimální čtecí vzdálenost maximálně do 30 cm. Tento typ RFID se nejvíce využívá u docházkových, stravovacích systémů. Slouží k identifikaci osob, čip je ve formě ID karty nebo klíčenky.

HF - Používá frekvenci 13,56 MHz, zde je už větší vzdálenost čtení. Vzdálenost čtení se nepřesahuje 1 metr. Využívá se ve výrobě produktů, k identifikaci produktů na běžícím pásu. Využití také v obchodech, systémy proti odcizení zboží

UHF – Používá frekvence 868/869 MHz pro Evropu. Vzdálenost čtení se pohybuje do 3 metrů. U technologie UHF čtení velmi negativně přítomnost kovů

MW – Používá frekvence 2,4 GHz a 5,8 GHz. Tato frekvence pracuje v blízkosti frekvenčního pásma Wi-Fi sítí, které jsou dnes skoro všude a stále se rozšiřují. Zde může docházet k vzájemnému rušení technologií. U MW technologie se čtecí vzdálenost pohybuje do 10 metrů. Nevýhodou této technologie je vysoká cena, rušení signálu v přítomnosti kapalin a kovů.

Dělení RFID podle napájecího obvodu:

Aktivní čipy – Aktivní čipy se hlásí sami jako první (TTF= tag talks first) čtečce a vysílají své informace do okolí. Nevýhodou je výdrž baterií, která se pohybuje kolem 1-5 let, baterie se musí měnit. Aktivní tagy mají čtecí vzdálenost až 100m, ale je zde velmi vysoká pořizovací cena. Paměť až 100 kB.

Pasivní čip – Hlásí se až na vyžádání čtecího zařízení (RTF = reader talk first). Pasivní tagy nemají vlastní baterii a jsou napájeny až z pole čtecího zařízení. Výhodou je, že je cenově přijatelnější než aktivní tagy. Čtecí vzdálenost se pohybuje od 0,5 m – 10 m. Paměť se pohybuje od 64 – 256 bitů. Výhodou je odolnost proti teplotám a fyzickému namáhání. Dlouhá doba životnosti.

Semi-aktivní – Mají baterii, která slouží pouze k napájení antény a tím se zvyšuje čtecí vzdálenost.

Semi-pasivní – Mají baterii, která slouží pouze k napájení mikročipu, nezvyšují čtecí vzdálenost.

Rozdělení čipů podle tříd:

Třída 0 – Pouze pro čtení, programování probíhá při výrobě. Mají 64 nebo 96 bitů. Rychlost čtení 1000 tagů za sekundu.

Třída 1 – Lze zapisovat jednou číst mnohokrát (WORM). Programuje se při použití. Paměť je o velikosti 64 nebo 96 bitů. Rychlost čtení 200 tagů za sekundu.

Třída 0+ - Lze zapisovat a číst mnohokrát (READ/WRITE). Programuje se kdykoliv. Paměť je o velikosti 256 bitů. Rychlost čtení 1000 tagů za sekundu.

Gen 2 - Lze zapisovat a číst vícekrát. Paměť o velikosti 256 bitů. Čtení 1600 tagů za sekundu.

2.3.4 Využití RFID

RFID nám pomáhá jedinečně identifikovat produkt, objekt, člověka a vše kolem nás. RFID nám nejen jednoznačně identifikuje objekt, ale také je schopen uchovávat o něm informace. Součástí RFID mohou být senzory, které nám sbírají data a uchovávají v paměti

RFID, například senzory teploty. RFID se dá využít téměř všude a nejen proto, že RFID je nástupce dnes všem známým čárovým kódům. Nejvíce se prozatím využívá v logistice.

RFID čipy mohou obsahovat i senzory. Senzory pohybu, otřesu, vlhkosti, teploty, polohy (GPS). Ty to senzory své údaje zapisují do paměti čipu a poté co jsou na dosah čtecího zařízení, se data přenesou do informačního systému.

Představme si, třeba výrobu osobního automobilu. Osobní automobil se skládá z mnoha dílů. Ve Stuttgartu kde se vyrábí automobily Porsche, jsou o každém voze vedeny informace. Jaké díly byly použity, kdo z automechaniků na autě pracoval a kdy. Zde bude časem možné, kdy každý výrobek bude mít svůj RFID čip. A bude vše fungovat jako skládačka, kdy se do informačního systému přidávají data o dílech. Po té bude zákazník vědět, z čeho se jeho auto skládá a zda nebyly použity nesprávné díly při výrobě auta.

2.3.5 řešení pomocí RFID

2.3.5.1 Přepravní firma

Představme si expresní přepravní firmu, která přepravuje zásilky po celém světě. Přepravní firma funguje tak, že zákazník zavolá na zákaznické centrum a poté dispečer vyšle kurýra na místo vyzvednutí zásilky. Zde je opatřen přepravním listem, kde je čárový kód. Pak se veze balík na depo kde je každý kus zvážen, změřena opatřen identifikačním štítkem. Zásilky se třídí podle cílové destinace. Tady je vše v pořádku, jestliže používáme čárové kódy. Jenže, při každém opuštění depa, překládání v překladišti nebo v cílovém depu se musí každý balík naskenovat. Tím se data přenášejí do informačního systému a zákazník ví, kde se právě zásilka nachází. Ale velké firmy mají velké množství zásilek a proto se skenováním zásilek stráví mnoho času. Čárový kód musí být každý zvlášť nastřelen, jestliže některá depa mají tenhle proces automatizovaný pomocí dopravních pásů, stále dochází k chybám čtení. Stačí, když je štítek špinavý a už se čárový kód nenaskenuje. Zavedením RFID se tyhle chyby čtení dají minimalizovat. Stačí se zásilkami projet přes čtecí brán a okamžitě se načtou do informačního systému a to i v případě, že zásilky jsou na sobě a RFID čipy nejsou vidět. Tohle ušetří firmě mnoho času a čas jsou peníze.

Taková by dnes nemohla existovat bez informačního systému. Každé skenování RFID čipu se nám zobrazí v systému, tím je zajištěna kontrola zásilek a sám zákazník si to

může ověřit a ví, kdy může počítat s doručení zásilky. V logistice má RFID určitě co nabídnout.



Obrázek 4 Schéma logistické firmy (GS1)

2.3.5.2 Hlídání majetku

Například firma TNT Express, využívá RFID pro kontrolu a sledování „Blue cage“, jsou to klece ve kterých se přepravují nepaletizované zásilky. Dříve nebo ještě v některých depech kde tato služba nefunguje, se každé pondělí dělala inventura. Klece mají čárové kódy, které se musejí skenovat. V Ostravě má TNT Express malé depo, kde každý den přijíždí jeden kamión, který v průměru vozí asi osm klecí denně. Ale ve velkých překladištích například v Německu ve městě Norimberk, zde je už mnoho přepravních klecí, které jsou naskládány za sebou a zde inventura může trvat i hodinu. Proto TNT express, zavedla RFID čipy od firmy AeroScout, tyto čipy jsou aktivní, mají v sobě baterii, pracují s Wi-Fi zařízením a není třeba žádných jiných čtecích zařízení pro RFID. Čipy RFID také obsahují senzory vlhkosti a teploty. Čipy vysílají co 30 min signál a hlásí se systému. Obsahují také kontrolní mechanismus, který hlídá kapacitu baterie. Když se životnost baterie chýlí ke konci, objeví se to v informačním systému a nastane výměna. Vzhledem k tomu, že čipy využívají Wi-fi zařízení, které je na každém depu dostupné z důvodů přenášení dat mobilních skenerů. TNT Express to ušetří mnoho času a navíc má přesné údaje kde se klece nacházejí a v jakém prostředí se nacházejí. Protože prostředí, ve kterém jsou zásilky přepravované, je taky velmi důležité.



Obrázek 5 Čip RFID od firmy Aeroscout

2.3.5.3 Nemocnice

Zde umožňuje firma AeroScout identifikaci pacientů, každý pacient je opatřen čipem, díky čipu je možné spravovat data o pacientech. Například kdy byla provedena vizita, kde se pacient nachází. Čipy obsahují i senzory teploty a vlhkosti. Díky informačnímu systému je možno vidět kdy byla provedena poslední vizita a po té automaticky zavolat lékaře na další vizitu. Velmi prospěšné je i řešení podávání léků pacientům, opět vše zpracovává informační systém. Představme si, že pacient bere tolik léků, že některé při vzájemném požití mohou vyvolat alergickou reakci, tohle také je kontrolováno informačním systémem. Monitorovány jsou také mobilní zdravotní zařízení EKG a jiné, jsou to velmi drahé přístroje, proto se vyplatí je kontrolovat a znát jejich polohu. Informační systém s pomocí RFID umožňuje zlepšení efektivnosti a přesnosti lékařského personálu.

2.3.5.4 Věznice

V USA se RFID čipy využívají k identifikaci vězňů. Čip je implantován do ramen. Ve věznicích v USA se kontroluje také poloha gangů ve věznici, aby nedocházelo ke krvavým incidentům. Vězni jsou monitorováni, aby neutekli a nezdržovali se na místech, která jim nejsou určena. Tento monitorovací systém se věznicím v USA vyplatí hlavně kvůli bezpečnosti obyvatel, ale i samotným vězňům.

Ve Velké Británii se testují RFID čipy pro lidi obviněných ze zločinů propuštěných na kauci. Dnes dostávají sledovací náramky a RFID je zřejmě nahradí.

V ČR se uvažuje o nasazení RFID čipů jako sledování osob, kteří byli odsouzeni k domácímu vězení.



Obrázek 6 RFID náramky pro hlídání vězňů

2.3.5.5 Plynárenská společnost

Představme si, kdysi se kontrola prováděla pomocí papíru a tužky, údaje se zapsali na papír a po té se teprve data zapisovali do informačního systému, kde byla zpracována. Dnes většina společností má na každém plynoměru identifikační číslo s čárovým kódem. Pracovník plynáren přijde s mobilním PDA zařízením, naskenuje čárový kód a vidí předchozí spotřebu, potřebné údaje o zákazníkovi. Zadá do skeneru aktuální spotřebu, ta se okamžitě pomocí GPRS² přenese do informačního systému, vše je kontrolováno. Pokud se pracovník plynáren překlepne a zadá velmi špatný údaj, informační systém vyhodnotí podle předchozí spotřeby data a v případě možné chyby upozorní systém pracovníka plynáren. Tyto čárové kódy se nahrazují RFID čipy, v budoucnu tyto čipy budou automaticky posílat data o spotřebě plynu a tím se ušetří čas a peníze vynaložené na mzdu pracovní plynáren.

² GRPS- Je mobilní datová služba přístupná pro uživatele mobilních zařízení, používá se k připojení k internetu a přenosu dat.

2.3.5.6 Mýtné brány

Pomocí RFID je možné identifikovat a lokalizovat vozidla pohybující se po dálnici nebo cestě které spadají pro placení mýtného. Každé vozidlo je opatřeno palubní jednotkou, která má v sobě obsažen čip. Palubní jednotka jednoznačně identifikuje vozidlo. Při vydání palubní jednotky se do systému zadávají data o vlastníkovi vozidla, o vozidle a řidičovi vozidla. Po projetí mýtnou bránou je odečtena částka z kreditu popřípadě připsána na účet vlastníka palubní jednotky. Zavedení mýtných bran stál mnoho peněz, ale je spočítáno, že návratnost investice se počítá na několik měsíců. Zavedení mýta přineslo státu mnoho peněz do státní pokladny.



Obrázek 7 Mýtná brána v ČR

2.3.6 Nebezpečí RFID

Velikou nevýhodou je, že čip v blízkosti silného elektromagnetického pole se může poškodit. Také zde hrozí útoky vysláním signálu „kill“, který byl původně vytvořen pro deaktivaci čipu, například po zaplacení zboží aby dále už nebylo možné sledovat čip. Ale v případě vyslání signálu „kill“ zlodějem by bylo možné odnést zboží bez zaplacení a nikdo by si toho nevšiml.

Dalším nebezpečí jsou útoky hackerů³, kteří jsou schopní do RFID čipu nahrát virus. A pomocí tohoto viru jsou schopni nakazit nebo i poškodit informační systém. Třeba si koupí v obchodě zboží, doma do čipu nahraje virus a po té se vrátí zpět do obchodu, kde

³ Hacker-Jsou to počítačové piráti, znají velmi dobře programové vybavení IT. Umí narušit systém a krást data.

danou věc koupil. Čtečka načte znovu RFID čip a s ním načte i virus a přenesse ho do systému. Tento systém představili na univerzitě v Amsterdamu.

Další nebezpečí spočívá v tom, že čtení probíhá bez kontaktně a tudíž se majitel nedozví, že byly načteny jeho data. Zde hrozí, že se citlivé informace dostanou do nesprávných rukou.

2.4 Překážky IoT

Není pochyb, že internet věcí je něčím novým a prozatím vývoj je na špičce ledovce. Internet věcí s novými technologiemi se bude rozrůstat velmi rychle. Ale je zde mnoho překážek jak technologických tak i humánních.

Aby Evropská Unie urychlila vyřešení překážek a nalezení problémů týkajících se internetu věcí vytvořila akční plán pro internet věcí.

2.4.1.1 Internet věcí: 14-bodový akční plán

1. Ovládání.

Komise bude pracovat na definici souboru zásad správy internetu věcí a návrh architektury musí být vybaven dostatečnou úrovní decentralizovaného řízení.

2. Soukromí a ochrana údajů.

Komise bude pečlivě sledovat uplatnění právních předpisů na ochranu údajů v Internetu věcí.

3. Právo na "mlčení čipů".

Komise zahájí diskusi o tom, zda jednotlivci by měli mít možnost odpojit se od svého síťového prostředí v každém okamžiku. Občané by měli být schopni přečíst základní informace v RFID (Radio Frequency Identification Devices) a v případě potřeby vyřadit čip, aby bylo zachováno soukromí uživatelů. Tato práva jsou patrně velmi důležité pro ochranu soukromí. RFID a další bezdrátové technologie staly neviditelnými a proto je ochrana údajů velmi důležitá.

4. Vznikající rizika.

Komise přijme účinná opatření k tomu, aby internet věcí plnil náročné úkoly spojené s důvěrou, přijetím veřejností a bezpečností.

5. Životně důležité zdroje.

V souvislosti se svou činností na ochranu kritické informační infrastruktury. Komise bude pozorně sledovat vývoj internetu věcí v životně důležitých zdrojích pro Evropu.

6. Normalizace.

Komise v případě potřeby zahájí další standardizační pověření spojené s internetem věcí.

7. **Výzkum.**

Komise bude i nadále financovat společné výzkumné projekty v oblasti Internet věcí, prostřednictvím rámcového programu.

8. **Veřejné a soukromé partnerství.**

Komise budou začleňovat, jako adekvátní, internet věcí ve čtyřech výzkumech a vývoje veřejno-soukromého partnerství, které se připravují.

9. **Inovace.**

Komise zahájí pilotní projekty na podporu připravenosti organizací v EU v oboru internet věcí. Efektivněji podpořit nasazení internetu věcí na trhu s ohledem na bezpečnost a soukromí, aplikací spojené s Internetem věcí.

10. **Institucionální povědomí.**

Komise bude pravidelně informovat Evropský parlament a Radu o vývoji internetu věcí.

11. **Mezinárodní komunikace.**

Komise posílí komunikaci o internetu věcí se svými mezinárodními partnery. Bude sdílet informace a osvědčené postupy a bude se snažit dohodnout na společné akce.

12. **Životní prostředí.**

Komise posoudí obtíže spojené s recyklací RFID tagů, stejně jaké výhody přinese přítomnost tagů na recyklaci různých věcí.

13. **Statistiky.**

Eurostat začne zveřejňovat v prosinci 2009 statistické údaje o využití technologií RFID.

14. **Vývoj.**

Komise bude shromažďovat a sledovat reprezentativní soubory evropských zúčastněných stran ve vývoji internetu věcí.

2.4.1.2 *Sdílení dat*

Nezbytné pro realizaci internetu věcí je sdílení dat, ale jde o sdílení většiny dat, ke kterým bude mít přístup kdokoliv. Zde internet věcí bohužel naráží na odpor některých lidí. Protože předměty budou obsahovat data a člověk, který jej používá, může o sobě

hodně prozradit. Zde je důležité zavést určitá pravidla, co a kdo bude mít přístup k datům. V případě zavedení celosvětového informačního systému by hrozilo nebezpečí, zneužívání postavení států ke zjišťování dat ve svůj prospěch. Navíc zde také hraje svoji roli rivalita mezi státy jako je Rusko a USA nebo jiné. O nebezpečí sdílení dat se budu zabývat v bodě 5.3 Nebezpečí IoT.

2.4.1.3 Standardizace

Standardizace v oboru internetu věcí je velmi důležitá, vize je taková, že budeme moci zjistit údaje o čemkoliv a na celé planetě Zemi. Jenže má to háček už dnes se například u RFID čipů používají ve světě různé frekvence. A proto zde je nutné, aby se státy domluvili na jednotných parametrech. Zřejmě nebude možné, aby všichni používali stejné jednotné frekvenční pásmo, ale bude nutné, aby čtecí zařízení byli univerzální a dokázali přečíst informace z jakéhokoliv čipu, ať už je z Číny nebo je vyroben v Evropské unii. Ale standardy je důležité dodržovat ve vývoji internetu věcí, aby byla hlavně zachována bezpečnost a funkčnost internetu věcí.

2.4.1.4 IPv6

Kdysi při vytvoření protokolu TCP/IP se nepočítalo, že se počítačové sítě dočkají takového rozmachu. Dnes má počítač skoro každá domácnost, aby byl počítač připojen k počítačové síti, musí používat protokol TCP/IP dnes nejvyužívanější a musí být nainstalován pro připojení k síti Internet. Každý počítač má přidělenou IP adresu. Dnes se používá nejvíce protokol IPv4, který používá 32bitové adresy, například: 192.168.0.1. Ale vzhledem k nedostatku IP adres byl vyvinut protokol IPv6, který používá 128bitové adresy. Adresa IPv6 se zapisuje jako osm skupin po čtyřech hexadecimálních číslicích, například: 2001:0718:1c01:0016:0214:22ff:fec9:0ca5. Protože Internet věcí počítá s připojením obyčejných věcí k síti Internet, aby každý objekt měl svou IP adresu je zavedení protokolu IPv6 nezbytné. Současná verze IPv4 nemůže nabídnout tolik IP adres. Takže velikou překážkou je zavedení protokolu IPv6.

2.4.1.5 WEB 3.0

Termín WEB 3.0 označuje další vývoj webu včetně architektury a aplikací. Jde o usnadnění vyhledávání informací a rozšíření funkcí webu jak ho dnes známe.

WEB 3.0 bude například obsahovat:

- **Implikace prvků sémantického webu.**

Dnes je web změt' stránek kde je problém najít relevantní informace. U sémantického webu jde o web, kde jsou informace uloženy podle standardizovaných pravidel a tím jsou informace lépe vyhledatelné. Jde například o to, aby každý obrázek, video obsahoval informace o autorovi, klíčová slova a podobně. Tuto standardizaci podporují i mikroformáty.

- **Mikroformáty**

Pro přiblížení mikroformátů si představme, navštívíme web nějaké firmy, zde se určitě dozvíme jméno, adresu firmy nebo telefonní kontakt. Lidé jsou schopni v textu vyhledat informace, které potřebují, ale počítač to neumí a k tomu mají pomoci mikroformáty. Jde o zapsání kódu v určitém formátu (mikroformátu).

Příklad : `<div class="street-address">Holečkova 12</div>`

`Praha 4 - Smíchov`

`Czech Republic`

První řádek počítači říká, že jde o ulici, druhý řádek poukazuje na město a třetí na název země.

Představme si, jsme členem nějakého klubu a na stránkách je seznam kontaktů a telefonních čísel. Dnes bychom těžce a časově náročně kopírovali a přepisovali kontakty do nějakého seznamu. Ale díky formátů zadáme příkaz a budeme mít okamžitě data v počítači nebo dokonce v mobilu. Takže mikroformáty umožňují pochopit počítačům to, co čteme a tím nám napomáhat k vyhledávání informací.

- **Sdílené aplikace**

Jde o sdílení dat, které můžeme sdílet ostatními uživateli internetu. Třeba sdílet své dokumenty námi vytvořené, které mohou pomoci ostatním. Tuto službu provozuje například GoogleDocs.

- **Přístup na web skrz aplikace pro různá zařízení.**

Samozřejmě dnes jsou lidé velmi v pohybu a jsou rádi připojení k síti Internet, ať už si čtou zprávy ze světa nebo chtějí být v kontaktu s kamarády pomocí sociálních sítí nebo různých komunikátorů (Jabber, ICQ, Skype). Proto je důležité, aby lidé měli přístup na web přes aplikace pomocí mobilních zařízení (Notebook, PDA, mobilní telefon).

- **Větší interakce na softwarové úrovni.**

V budoucnu by měl být schopen vytvořit program kdokoliv. Dnes je už mnoho nástrojů, které se snaží programování usnadnit, ale stále je nutnost znát programovací jazyk. Proto zavedení nástrojů, které umí

vytvořit program podle představ uživatele a to i bez znalostí programovacího jazyka.

- **Dotazování v přirozeném jazyce**
- **Částečná umělá inteligence webu**
- **Větší využití videa**
- **3D prostředí webových prohlížečů**

2.4.1.6 Bezpečnost IoT

Internet věcí v budoucnu bude řídit pro lidstvo nezbytné procesy, jako je výroba elektrické energie, řízení dopravy na cestách, výroba plynu, rozvod tepla do domácností. Jakákoliv chyba v kritických odvětvích by mohla znamenat velmi vážnou situaci. Například si představme z nějakého důvodu „spadnutí“ systému a najednou nebude v domácnostech a všude kolem elektrická energie. Kdyby se například ocitla Česká republika na týden bez elektrické energie, systém by se zhroutil. Zavládl by chaos a panika, lidé by začali rabovat a mohlo by docházet i ke ztrátám na životech. K takové situaci nesmí nikdy dojít.

Proto je kladem velký důraz na bezpečnost internetu věcí. Proto je důležité, aby na vývoji IoT dohlížel státní sektor.

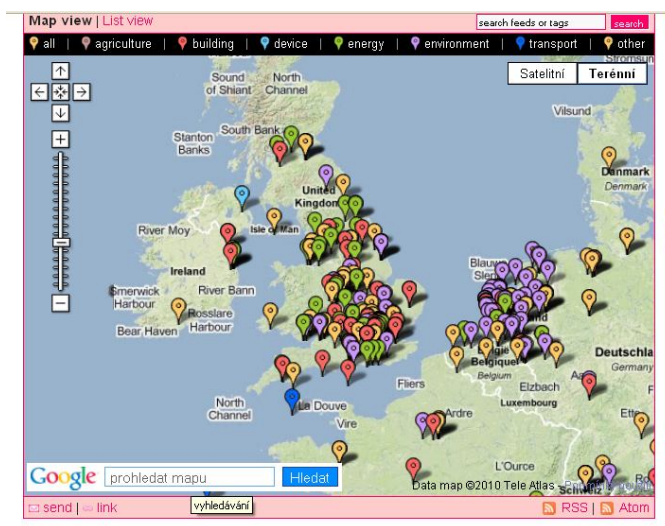
2.5 IoT dnes

Internet věcí se hodně rozrostl s příchodem čipů RFID. Rok 2009 byl pro internet věcí zlomový, bylo představeno mnoho produktů. Pár vybraných produktů si přiblížíme.

2.5.1 Pachube.com

Pachube byl představen teprve nedávno a je stále v testování, je to systém, který se snaží o celosvětový informační systém. Pachube umožňuje zaznamenávat a sdílet data v reálném čase od senzorů, budov a různých objektů. Kdokoliv může připojit zařízení do IS Pachube. Pachube je postavena také na mapách Google. Pachube prozatím tvoří hlavně vývojáři a připojují své senzory k síti. Po připojení do sítě Pachube uživatel vidí mapu a na ní jsou označeny body, které zobrazují různé senzory, objekty a zařízení. Pachube má rozdělené senzory na zemědělství, budovy, zařízení, energie, životní prostředí a doprava. Navíc dnes mobilní telefony jdou technologicky velmi kupředu a obsahují v sobě mnoho senzorů. Obsahují senzory teploty, pohybu, mají mikrofón, mají kamery a obsahují GPS. I tyto senzory například u iPhone se dají pomocí aplikace připojit. Ale Pachube nepočítá jen

s tím, že bude zobrazovat data senzorů, ale jeho vizí je vzdálené ovládání různých zařízení a objektů. Pachube je postavené na bezpečných protokolech a přístup k zařízení je šifrován. Pomocí Pachube bude možné, si otevřít dveře od své garáže. Dnes se můžeme připojit k internetu odkudkoliv a tím nám Pachube umožňuje ovládat věci odkudkoliv na Zemi, kde je připojení k internetu. Pachube je systém postavený pro realizaci internetu věcí.



Obrázek 8 Informační systém Pachube

2.5.2 IBM řešení pomocí senzorů

IBM je jedna z největších IT firem a také v internetu věcí. Nabízí mnoho RFID a technologické řešení senzorů. IBM spolupracuje s různými výrobci a dodavateli zboží. IBM od února 2010 navrhlo senzorové řešení pro Container Centralen. Tento systém má sledovat pokrok přepravy od pěstitelů pro velkoobchody a maloobchody v celé Evropě. IBM má také dohodu s Matiq, je to dceřiná společnost největšího norského dodavatele jídla Nortura. Projekt zahrnuje použití RFID technologie pro sledování a dohledání drůbeže a masných výrobků z farmy a to až do regálů supermarketů. Toto sledování jídla pomůže zajistit, aby výrobky byly udržovány v optimálním stavu. IBM velmi usilovně dostává internet věcí do podvědomí lidí. Vydali mnoho videí a také mnoho reklam, které upozorňují a propagují budoucnost internetu věcí.

2.5.3 Arduino

Arduino je open source ⁴platforma elektronických prototypů. Skládá se z open source software a hardware. Je určena pro vývojáře, konstrukční inženýry, fandy IT a zájemce o vytváření interaktivních objektů. Hardware Arduino se dá vytvořit ručně, nebo se dá koupit smontované a otestované, vypadá jako základní deska počítače jen o něco menší. Arduino je schopné vnímat okolí pomocí různých senzorů, ale také je schopné jej ovlivňovat pomocí led diod, motorků dalšími výstupními periferiemi. Arduino se dá koupit i u nás, cena se pohybuje kolem 700- 1200 Kč. Toto zařízení se připojí přes USB k počítači nebo existuje „Arduino Ethernet Shield“ pomocí tohoto zařízení připojíte své Arduino ke své počítačové síti pomocí standardního konektoru RJ-45 ⁵. Software je ke stažení zdarma a programování je jednoduché a je založeno na programovacím jazyku Wiring, který je podobný jazyku C.

Tato zařízení mohou dělat cokoli, záleží jen na fantazii a šikovnosti. Na internetu se nachází mnoho návodů. Například je možné kontrolovat teplotu ve skleníku a data odesílat na sociální síť Twitter⁶.

Výhody Arduino spočívají v jednoduchém programování, zapojení, nízká cena proti jiným kitům, uživatelská komunita, spousta návodů zdarma a platformní nezávislost (Windows/Linux/MacOs).



Obrázek 9 Arduino

⁴ Open source- Je počítačový software s otevřeným zdrojovým kódem. Otevřenost zde znamená jak technickou dostupnost kódu, tak legální dostupnost licence software.

⁵ Konektor RJ-45- Je dnes nejčastěji používaný typ zapojení ethernetových kabelů UTP.

⁶ Twitter- Je poskytovatel sociální sítě a mikrobloggeru, který umožňuje uživatelům posílat a číst příspěvky zaslané jinými uživateli.

2.5.4 Fedex senseaware

Mezinárodní kurýrní firma Fedex zprovoznila nové sledovací zařízení balíků a nové služby na webu. Sledovací systém udržuje přehled o teplotě, umístění a zacházení s balíkem. Systém je dokonce schopen zjistit zda byl balík po cestě otevřen. Tento systém je v testovací fázi. Prozatím se kontrolují zásilky zdravotnického zařízení a dokonce i lidských orgánů a tkání.

2.5.5 Violet

Je francouzská firma, která se snaží přinést internet věcí do domácností pomocí svých produktů. Svými produkty se snaží automatizovat procesy, které se denně opakují. Tyto produkty využívají také RFID čipy. Violet udává na trh hlavně dva produkty Mir:ror a králíčka Nabaztag.

Mir:ror

Mir:ror vypadá na první pohled jako malé zrcadlo s připojením k počítači. Jedná se hlavně o RFID čtecí zařízení. Při zakoupení produktu dostanete toto malé zrcadlo a mnoho „Ztamp“ což jsou RFID čipy uložené v plastových nálepkách. Ale také software, který tvoří hlavní nápad a dává duši produktu. Tento produkt funguje tak, že své osobní věci, které denně používáme, označíme je Ztamp. Tím je jednoznačně identifikujeme. Dále je na naší fantazii jak proces spjatý s naší věcí naprogramujeme.

Například označíme si náš deštník. Ráno každého z nás určitě zajímá, zda bude pršet a zajímá nás předpověď počasí. Proto mámě několik možností zapne si televizi a podíváme se na zpravodajství nebo si vyhledáme počasí na internetu a poté vyhledáme počasí v našem městě. Tuto činnost denně opakujeme a zabírá nám čas, proto stačí tento proces naprogramovat k našemu deštníku. Při odchodu z domu stačí přiložit deštník k zrcadlu a nám se okamžitě ukáže počasí na počítači a v našem městě.

Další příklad může sloužit k identifikaci k počítači. Počítač v domácnosti používá celá rodina a každý uživatel má vytvořen svůj profil, který je opatřen heslem. Přilepíme si Ztamp na předmět který stále nosíme u sebe, peněženku nebo mobil. Místa zadávání hesla a vybírání profilu stačí přiložit Ztamp k zrcadélku a rázem jsme připojeni.

Ale pomocí předmětů může sdělovat i své pocity nebo události na sociální síť. Přilepíme si Ztamp na náš hrníček od kafe a po každé kdy si uděláme kafe, stačí položit hrnek na zrcadlo a na Facebooku se nám zobrazí náš status, například: právě mám pauzu na kafe.



Obrázek 10 Mir:ror od firmy Violet

Nabaztag

Nabaztag je malý roztomilý elektronický králíček, který má stejné funkce jako Mir:ror, ale také mnoho funkcí navíc. Obsahuje čtečku RFID čipů, mikrofón, reproduktor a obsahuje Wi-Fi připojení. Umí číst E-mail ve 35 jazycích. Přehrává hudbu z internetových rádií nebo naší hudbu uloženou v počítači například v mp3. Detekuje RFID čipy a na základě rozpoznání provede naprogramované akce. Poslouchá i hlasové příkazy. Funguje, i když je počítač vypnutý.

Nabaztag je malý společník, který nás může pobavit, ale i ušetřit mnoho času. Představme si, že ráno vstáváme a mezitím co si děláme snídani, nám malý rozkošný králík poví, jaké bude dnes počasí, podle toho se začnete oblékat a posloucháte jaká je dopravní situace na cestách. Nebo si necháte přečíst, co se stalo ve světě z internetových novin a vaše zprávy na internetu. Tím nám Nabaztag ušetří mnoho času. A bude nám věrným společníkem.



Obrázek 11 Králíček Nabaztag od firmy Violet

2.5.6 WideNoise

Jak už jsem se zmiňoval dnešní mobilní telefony jako Iphone obsahují mnoho senzorů. Widenoise je aplikací pro Iphone, která měří hladinu decibelů hluku na daném místě. Tyto data posílá do systému, kde je ostatní uživatelé mohou sledovat. Můžete například zjistit, jestli žijete v klidném prostředí a v době potřeby klidné relaxace můžete vyhledat klidné místo v přírodě. Tento projekt je zajímavý, i když toto měření hluku není velmi přesné, jedná se o projekt, který se snaží propojit přístroje s internetem.



Obrázek 12 Aplikace WideNoise

2.6 Budoucnost IoT

Budoucnost Internetu věcí, která nás čeká, si neumíme dnes ani představit. Vše co jsme viděli ve Sci-Fi filmech se časem stane skutečností. Vývoj technologií je velmi rychlý. Počítače zvětšují výkon a svojí datovou kapacitu. Věřím, že v budoucnu bude každý předmět vysledovatelný přes satelit. A každý předmět bude propojen s internetem nejen, že předměty budou o sobě podávat data, ale budou se moci i na dálku řídit. Další budoucnost Internetu věcí se budu snažit nastínit v bodech 3.4 řešení distribuovaného IS v IoT v budoucnu a 4.3 řešení izolovaných IS v IoT v budoucnu.

3 IoT jako distribuovaný informační systém

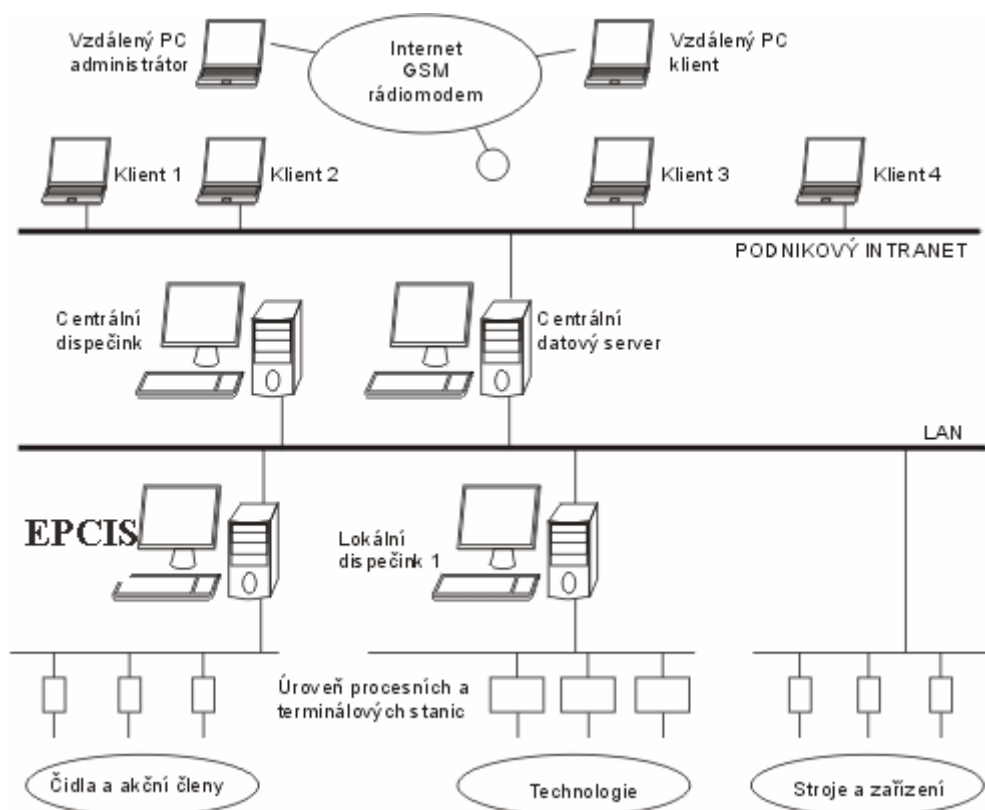
IoT jako distribuovaný jako takový, teprve vzniká. Aby internet věcí fungoval, jako distribuovaný systém je nutné, aby všichni sdíleli svá data a své zařízení. A tady distribuované systémy naráží na neochotu spolupracovat některých firem a uživatelů zařízení.

3.1 Co je distribuovaný IS

Distribuovaný systém se skládá z více autonomních uzlů, tyto uzly se navenek jeví jako jeden systém. Tyto uzly pracují společně na řešení problému (procesu). Distribuované systémy se začali zavádět u počítačů. Při velkých výpočtech by operace trvala jednomu počítači tehdy s jedním procesorem velmi dlouho a proto se počítače propojovali do tzv. „počítačových farem“. Tyto farmy pracovali společně na jednom výpočtu tak, že se jeden proces rozdělil na části a každý počítač pracoval na části procesu. Tyhle počítačové farmy využívala a využívá hlavně NASA a vědecké výzkumné střediska.

U distribuovaných systémů je důležité, aby každý uzel sdílel své prostředky jak hardware, tak i data uložené v něm (databáze, aplikace). Každý uzel musí být přístupný a schopný spolupracovat a komunikovat s ostatními uzly. Systém musí být odolný proti chybám, v případě že bude nefunkční jeden z uzlů je potřeba tohle zjistit vyhodnotit a proces, který prováděl daný uzel převést na jiný, tak aby systém zůstal funkční nebo aspoň pracoval omezeně.

3.2 Struktura distribuovaného IS



Obrázek 13 Schéma distribuovaného systému

Zde vidíme strukturu distribuovaného systému a propojené od senzoru přes EPCIS a různé servery až po připojení přes internet.

3.3 Výhody distribuovaného IS

Výhody distribuovaných systému spočívá v tom, že systémy sdílí svá data a hardware všem v okolí. A celý systém se skládá z více malých spolupracujících systémů. Vyřazení jednoho uzlu neohrozí pád celého distribuovaného systému. Buď bude systém pracovat omezeně nebo omezení ani nepoznáme. Například budeme všichni využívat celosvětový Informační systém. Při narušení nějaké podsystému někde v Japonsku, uživatel v české republice nemusí vůbec pocítit.

3.4 Řešení distribuovaného IS v IoT v budoucnu

Distribuované systémy nahrávají politice internetu věcí. Sdílet data, hardware ve prospěch lidstva.

3.4.1 Celosvětový IS

Mohli jsme vidět v mnoha sci-fi filmech kdy lidé komunikovali jen s jedním informačním celosvětovým systémem, který jim podával informace. Věřím, že takový systém v budoucnu bude existovat, Technologie jsou už dnes v dosahu. Díky RFID je takový informační systém možno vytvořit. Představme si systém s názvem Global IS, který bude fungovat na webu. U počítače, budou RFID čtečky. Výrobce vytvoří výrobek, označí jej RFID čipem a informace o tomto daném produktu ale i kusu zapíše do Global IS. Tím by všechny vyrobené výrobky, produkty byly na internetu. Koupíme si v obchodě nový kávovar a načteme si informace o produktu pomocí Global IS. Zde najdeme například manuál, jak zacházet s kávovarem nebo informace o součástkách a materiálech jaké kávovar obsahuje. Ale na stránkách bude i návod jak udělat nejlepší kávu v popřípadě se zde otevírá prostor i pro reklamu na určitou a doporučenou kávu. Ale to vše je jen vize do budoucnosti. Ale pro sdílení všech dat svět ještě není připraven a v dohledné době asi ani nebude. Každý si střeží své výrobní data a také některé data jsou pro firmy smrtelně důležité, jako třeba data zákazníků.

3.4.2 Pachube

Pachube je systém, který existuje dnes ve fázích testování, ale i když zrovna tenhle systém možná se neuchytí, protože je určen prozatím hlavně pro nějaké fanoušky elektroniky. Ale jestliže dojde k zjednodušení připojení předmětů k internetu, tak tento systém zažije velký nárůst uživatelů. Tento systém je příkladem distribuovaného systému. Pachube zastřešuje mnoho malých systémů, který sdílejí svá data, ale i svůj Hardware. Uvidíme, jestli se tento systém uchytí, bohužel jsou zde i rizika zneužití této technologie. O nebezpečí IoT se budu věnovat v bodě 5.4.

3.4.3 Systém bezpečnosti provozu

Už dnes se do automobilů montují krátkodosahové radary, které slouží k zjištění pekáček před vozidlem. Od roku 2013 mají být tyto radary povinnou výbavou vozidel v Evropské unii. Dnes mnoho aut obsahuje tempomat⁷, jedeme po dálnici, máme spuštěný tempomat, který pomocí radarů bude schopen regulovat vaši rychlost a vaši vzdálenost od vozidla, které jede před vámi. Protože nejvíce nehod je způsobeno nedodržením bezpečné vzdálenosti, díky tomuto systému by došlo ke snížení nehod. Ale v budoucnosti budou

⁷ Tempomat- Je zařízení sloužící k udržování nastavené rychlosti vozidla.

všechny auto spolu komunikovat. Jede řada aut za sebou a v okamžiku kdy se u prvního vozu objeví překážka, zpomalí a dá vědět pomocí systému zprávu autům za sebou, že mají zpomalit popřípadě zastavit. Tento systém, může rychle reagovat na nehody a automaticky odklánět dopravu po alternativních cestách, ještě dříve než dojde policie. Tento systém by snížil jak nehodovost, ale také by snižoval riziko vzniku dopravní zácpy. Opět takový systém přispěje k bezpečnosti provozu, ale v případě nabourání „hackerů“ do systému, by mohl nastat dopravní kolaps.

Auto před překážkou automaticky zpomalí nebo úplně zastaví a auta za ním také.



Obrázek 14 Systém bezpečnosti dopravy v budoucnosti

3.5 Zhodnocení

Distribuované systémy jsou budoucnost pro internet věcí. Tyto systémy budou v budoucnu lidé využívat jako hlavní zdroje informací. Distribuované systémy se budou starat o sledování, bezpečnost, přístup k informacím a zjednodušení našeho všedního života. Tyto systémy budou spojovat celý svět.

4 IoT jako lokální (izolovaný) informační systém

Jsou to systémy, které je určeny jen pro určitou skupinu uživatelů nebo jsou určeny pro určitou funkci. Například systém užívající uživatele určité firmy, sledovací zařízení aut. Systém určený pro ovládání našeho domu. Nebo sledovací systém zásilek přepravní společnosti.

4.1 Struktura Izolovaného systému IS

Dům na obrázku nám představuje izolovaný informační systém. Tento dům je izolován od ostatních domů a tvoří samostatnou jednotku.



Obrázek 15 Izolovaný systém domu

4.2 Výhody izolovaného IS v IoT

Výhody izolovaných systémů spočívá v určité izolovanosti od jiných okolních systémů. A tudíž narušení okolních systémů nebude mít vliv na náš izolovaný systém. Tento systém pracuje jako samostatná jednotka a pokud dojde k poruše je tento systém celý nefunkční.

Velkou výhodou je, že nesdílí své data a svůj hardware ve prospěch ostatních cizích uživatelů. A tyto izolované systémy, chrání naše soukromí.

4.3 Řešení izolovaných IS v IoT v budoucnu

Dnešní vývoj internetu věcí naznačuje a říká nám, co bude možné v budoucnu. Že pomocí internetu budeme moci ovládat cokoli. Takový izolovaný systém se bude snažit nastítnit, jak bude podle mě vypadat například v domech, kde žijeme a bydlíme.

4.3.1 Ovládací systém domu

V budoucnu si umím představit systém, kterým budeme ovládat náš dům. Věci v našem domě budou všechny propojeny a bude je spravovat náš systém. Pomocí aplikace v mobilu, počítači nebo budeme mít zavedený komunikátor v autě, budeme moci ovládat náš dům. Má to spoustu výhod. Jedeme například v zimním období ven. Systém přestane z důvodů šetření energie vytápět dům. Když budeme znát datum a čas návratu, stačí ho

sdělit systému a ten automaticky vytopí dům na dobu, kdy se máme vrátit. Co takový systém bude dále umožňovat?

4.3.1.1 Bezpečnost

Bezpečnost domu bude hlídat bezpečnostní systém. Alarm se automaticky zapne při odchodu uživatele. Systém bude sám kontrolovat osoby přicházející k domu a ohlašovat návštěvy. V případě pokusu o vnik, systém sám rozpozná pachatele a zavolá polici nebo zavede obranná opatření. Bezpečnost osob a majetku je jednou z výhod internetu věcí.

4.3.1.2 Efektivní využití elektrické energie

Protože jsou všechny zařízení propojeny, může je systém zapínat a vypínat, aby došlo k efektivnímu využití elektrické energie. Lidé si neuvědomují, že když zapnou své elektrické spotřebiče, dochází k přetížení elektrické sítě. Využití spotřebičů by řídil systém domu. Například by navrhl, kdy se budou zapínat určitá zařízení. Například pračka se zapne, v 10h a až dopere, zapne se mytí nádobí a jindy zase zavlažování trávníku. Tyto systémy by mohli pomoci rozdělit využití elektrické energie a zmírnit následky přetížení ve špičce.

4.3.1.3 Ekologické chování

Systém bude sledovat a hlídat například využití vody, energie, ztráty tepelné energie. Systém bude monitorovat využití vody a bude se snažit pomoci uživatelům ušetřit spotřebu vody a tím, že systém zaznamená zbytečně tekoucí vodu, která není využita, jednoduše zastaví kohoutky. Systém může sledovat otevření oken z důvodů vytápění a tepelných ztrát. Systém při vytápění zjistí, že někdo zapomněl zavřít otevřené okno. Systém jednoduše upozorní na otevřené okno a pak uživatel dá pokyn k zavření okna nebo jej sám zavře. Systém bude také napomáhat k recyklaci a třídění odpadů. V budoucnu bude mít každý výrobek RFID čip. Třídění odpadů je z důvodů recyklace velmi důležité a Evropská unie klade na recyklaci velký důraz. Doma budeme mít koše rozdělené podle materiálů (papír, plast, tetrapak, sklo). Budete chtít vyhodit plastovou láhev a náhodou uděláte chybu a budete chtít hodit láhev do nádoby určenou pro papír. Systém podle RFID čipu zjistí, o jaký výrobek se jedná a z jakého materiálu je složen a okamžitě upozorní na chybu. Internet věcí by lidstvo naučil třídění odpadků už doma a ušetřilo by se mnoho času

při probírání směsného odpadu. Věřím, že internet věcí naučí lidstvo se chovat ekologicky a to protože to je ve prospěch lidstva.

4.3.1.4 Komfort

Internet věcí ušetří hlavně mnoho času a zpříjemní nám lidem život. Mnoho procesů lidé vykonávají denně a internet věcí může pomoci s plánováním daného procesu nebo proces může vykonat za člověka. Například člověk vstává každý pracovní den a vstává do práce. Ráno vstane, jde si udělat kávu, zjišťuje předpověď počasí, obléká se a jede do práce. Pro systém nebude problém naplánovat různé procesy podle vás. Večer když půjdete spát, si nastavíte budík, systém vyhodnotí, že člověk bude vstávat v sedm hodin ráno. Aby ušetřil čas uživateli systému, sepne kávovar o 10 min před zazvoněním budíku, kontroluje předpověď počasí a to poví uživateli. Je zima a máme zamrznuté auto, systém zařídí rozmrazování auta a uživatel přijde rovnou do rozmraženého a vytopeného auta. Internet věcí nám ušetří mnoho času stráveného zbytečnými věcmi a bude mít více volného času a více času na relaxaci a odpočinek v dnešní uhoněné době.

4.4 Zhodnocení

Využití izolovaných systémů v internetu věcí má určitě velkou budoucnost i přes to, že internet věcí má spíše vizi, že všichni lidé budou mít informace o všem. Systémy nám ušetří mnoho času a budou vést k zpříjemnění našeho života. Výhodou izolovaných systému je, že sice umožňují ovládání různých věcí přes internet, ale jen určité skupině lidí nebo jednotlivci.

5 Srovnání funkcí IoT

Internet věcí zajišťuje nespočet funkcí. Největší význam je určitě ve sběru a zpracování dat z našeho okolí. Dále vše na Zemi bude sledovatelné, čím se na světě eliminují krádeže. Internet věcí se skládá z mnoha funkcí, ale ne všechny se dají brát jako pozitivní. A některé funkce se dají zařadit jak mezi pozitivní tak i mezi negativní.

5.1 Kladné funkce IoT

5.1.1 Sledování produktů

Internet věcí umožňuje sledovat, produkty kde se nacházejí. Na jakém místě a v jakém prostředí. Tato kontrola nad vyrobeným zbožím je velmi důležitá pro výrobce. Monitorování zboží eliminuje krádeže zboží, kterým dochází dnes všude a způsobuje velké finanční ztráty. Sledování produktů bude možné po celém světě. Sledovat budeme moci věci, výrobky, zařízení nebo i lidi.

5.1.2 Ovládání věcí přes internet

Velmi užitečné bude využívání funkce řízení věcí a zařízení přes internet. Tato funkce patří mezi kladné protože, umožňuje ovládat námi určené věci na dálku. Zapnutí naplněné pračky na dálku. Otevření oken domu z důvodů větrání. Ovládání lednice, zjištění co obsahuje a co máme dokoupit. Nebo budeme komunikovat se svým domem jako celkem, který nás bude informovat co se v domě děje a upozorňovat nás na různé chyby. Internet věcí umožní ovládání věcí a zařízení přes internet a to nám ušetří mnoho času a také fyzické námahy.

5.1.3 Informovanost

Hlavní důvod proč internet věcí vzniká, je zaznamenávání dat ze senzorů a sdílení těchto získaných dat. Sdílením těchto dat umožňujeme získávat informace ostatní lidem. Internet věcí zlepší a zpřesní informovanost v celém světě. Dnes když se díváme na po

5.1.4 Bezpečnost světa

Internet věcí může přinést, bezpečí do našeho života. Díky kontrolním systémům, které budou sledovat objekty. Internet věcí v budoucnu eliminuje počet dopravních nehod na minimum. Internet věcí může napomáhat varovat před přírodní katastrofou, pomáhat při evakuaci a zmenšit riziko ztráty na životech. Internet věcí může pomoci v boji proti terorismu. Kdyby každý člověk měl implantován RFID čip, byla by možná, nezaměnitelná identifikace člověka.

5.2 Rizika IoT

Každá technologie přináší užitek, ale také svá rizika. Dnes největší rizika v IT technologii, je hlavně odcizení a zneužití osobních údajů. Internet věcí prozatím přináší mnoho rizik, proto bohužel vývoj internetu věcí stagnuje. Jedná se hlavně o bezpečnost dat a právo na soukromí, ale také nebezpečí poruchy při řízení kritických procesů, jako je třeba výroba elektrické energie.

5.2.1 Ohrožení kritických procesů

V budoucnu bude každé zařízení připojené k internetu. To může mít fatální následky. Dnes největší riziko na internetu, tvoří hackeři, viry a spamy. Zde hrozí nabourání hackerů do systému, to může znamenat, omezení nebo odstavení systémů výroby elektrické energie. Zde by došlo k chaosu. Dnešní svět si bez elektrické energie nedokážeme představit. Proto řízení kritických procesů by mělo být izolováno a musí zde být zajištěna vysoká bezpečnost.

5.2.2 Narušení soukromí

Budoucnost RFID nám d života přinese mnoho ulehčení, ale také je zde vysoké narušení našeho soukromí. Představme si, že pro ulehčení nakupování budou všechny výrobky osazeny RFID čipy. Tento čip bude obsahovat každý předmět, objekt nebo zařízení. Čipy by mohly být marketingový nástroj. Nebezpečí spočívá v tom, že si koupíme oblečení a každý kdo má čtecí zařízení, by mohl zjistit, co na sobě právě máme. Tuto záležitost se snaží RFID čipy, řešit tak, že po zaplacení, by se čip dal deaktivovat. Dokonce byly návrhy, aby peníze obsahovali RFID čip. Zde by hrozilo nebezpečí, že kdokoliv by mohl vědět, kolik peněz máme právě u sebe. Díky čipům, bychom se stali vysledovatelnými, díky předmětům, které stále nosíme u sebe, peněženka, mobilní telefon. Mobilní telefon aniž bychom si to uvědomovali, tak i dnes zapnutý mobil je vysledovatelný a určuje naši polohu. I tohle je určité narušení našeho soukromí. Někteří lidé už vyjádřili svojí myšlenku, aby každý člověk byl už od narození opatřen čipem. Ovšem každý z nás si chrání své soukromí různým způsobem.

5.2.3 Nebezpečí terorismu

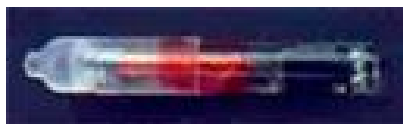
Zde by mohlo docházet k novému druhu terorismu, díky ovládnutí věcí přes internet. Například vyřazení systému letového provozu, by mohlo ohrozit během chvíle několik tisícovek lidí, právě cestujících v letadlech. Tento druh IT terorismu, by umožňoval ochromit svět ve větším globálním měřítku. Tak velký globální informační systém nebude snadné důrazně kontrolovat.

5.2.4 Humánní hledisko

Dnešní IT technologie umožňují sledovat věci v reálném čase. Ale technologie neumožňují sledovat jen věci, ale sledují také nás lidi. Dnes, kam se podíváme, můžeme spatřit kamerové systémy, na ulicích, na benzínové stanici, u bankomatu, v obchodech, na křižovatkách, ve výtahu a vůbec všude kolem nás. Tyto systémy mají hlavně bezpečnostní charakter a není pochyb, že podporují bezpečnost kolem nás.

Kamerové systémy jsou velmi rozšířené ve Velké Británii, tyto kamery jsou umístěny na ulicích, na letištích a na veřejných místech. Tyto systémy jsou schopné detekovat osobu a zaměřit její obličej. Po té systém vyhledává obličej ve své databázi a zjistí, o jakou osobu se jedná. Tyto systémy se využívají pro naši bezpečnost, snaží se vyhledat osoby hledané policií nebo napojené na teroristy. Hodně politiků z důvodu bezpečnosti jsou pro to, aby lidé měli implantován čip. To by urychlilo identifikaci lidí veřejných místech a zvýšila by se bezpečnost. Politici nás straší terorismem a snaží se prosadit různé zákony, mám strach, že jednou opravdu budeme muset nosit čipy.

Je to můj názor a možná trochu sobecký, ale nechci být monitorován na každém kroku a nechci, aby každý věděl, co právě dělám i přes to že by to znamenalo větší bezpečnost světa. Myslím si, že teroristé si najdou vždy nějaký způsob jak technologii obejít. Proti RFID čipům a proti sledování lidí jsou různé organizace například: www.spychips.com a www.dubistterrorist.de. Dlouho lidé bojovali za demokracii a svobodu slova, proto si myslím, že si ji tato práva nesmíme nechat vzít.



Obrázek 16 Čip určený pro implantaci do ramene

6 Závěr

Má bakalářská práce se zabývá technologií Internet věcí. Má práce je vizionářského charakteru, protože internet věcí teprve vzniká. Práce představuje tuto novou technologii z více pohledů.

V první části informuji, jak vypadá Internet věcí dnes. I když si to neuvědomujeme, každý z nás se určitě s internetem věcí setkal, ale ani nevíme, že daná věc spadá do technologie internetu věcí. Například na webu Českých drah, lze zjistit aktuální polohu vlaku a zda má zpoždění či ne.

Internet věcí udělal velký pokrok díky RFID čipům, které umí jednoznačně identifikovat předmět, výrobek, zvíře nebo člověka. Tyto čipy se dne nejvíce využívají v logistice pro sledování pohybu zásilek. RFID čipy mohou být osazeny různými senzory. Běžně se používají senzory pohybu, vlhkosti, teploty nebo otřesů. Dnes právě díky výrobcům a dodavatelských firmám se internet věcí nejvíce vyvíjí.

IT firmy vidí v internetu věcí budoucnost a také svůj business. Například jedna z největších firem IBM vsadila na výzkum nových technologií a prosazuje jejich nasazení v praxi. IBM vytvořila zajímavou reklamní kampaň, kde se snaží lidem představit budoucnost IT technologií a právě internetu věcí. IBM vyrábí a spolupracuje na řešení pro firmy, které chtějí využívat RFID technologie. V USA se o rozvoj RFID zasloužil obchodní řetězec Walmart, ten požaduje po svých dodavatelích, že musí používat RFID čipy. V obchodech vidím, že se jednou mnoho změní. Koho dnes baví vyndávání věcí z nákupního košíku? V budoucnu prostě projedeme kolem pokladny a zaplatíme samozřejmě elektronickou cestou zboží a budeme pokračovat k autu. Díky této technologii v obchodech zmizí fronty u pokladen a také i obsluha. O přípravu lidí na tuto technologii se snaží Obchodní řetězec Tesco, který se snaží zavést samoobslužné pokladny.

Internet věcí samozřejmě není jen o RFID čipech, Internet věcí má za úkol nejen sbírat informace o objektech, ale má umožnit také dané objekty pomocí internetu řídit. Toto dnes už umožňuje zařízení, známe jako Arduino, které se dá naprogramovat k ovládání téměř čehokoliv. A další využití tohoto zařízení umožňuje Informační systém Pachube. Pachube je distribuovaný informační systém, který propojuje všechny objekty na celém světě a umožňuje jejich ovládání nebo prohlížení jejich dat.

Internet věcí je bezesporu technologií budoucnosti, ale každá nová technologie přináší svůj přínos, ale také svá úskalí a problémy. Internet věcí v budoucnu udělá svět v některých odvětvích bezpečnější. Bezpečnější bude automobilní doprava, ale také bude těžké věci odcizit, protože každá věc bude sledována.

Dnes státní orgány, některé své praktiky monitorování lidstva se snaží zdůvodnit nebezpečím terorismu. Ve Velké Británii existuje mnoho kamer, monitorují různé místa obchody, letiště, dopravu na silnicích, vstupy budov. Aniž si to uvědomuje i my jsme na každém kroku monitorováni. Kamerové systémy dnes umějí podle obličeje vyhledat a rozeznat člověka a údaje o něm zapsané v databázi. Tato a jiná zabezpečení jsou důležitá, ale státy a bezpečnostní orgány mají jinou vizi. Už někteří kvůli „naší bezpečnosti“ navrhovali, aby byli čipy RFID implantovány každému člověku. Ale řekněme si, chceme, aby státní orgány sledovali náš pohyb a tím věděli o nás skoro vše? Tím to problémem se zabývají různé asociace. A zajímavou kampaň můžeme shlédnout na stránkách www.dubistterrorist.de. Můj názor je, že by měla být zachováno soukromí osob i přesto, že by to mělo znamenat menší bezpečnost světa. Já osobně jsem proti čipování lidí.

Internet věcí je technologie, která nám zpříjemní a mnoho ulehčí náš život. Díky této technologii ušetříme mnoho času a dojde k zefektivnění práce.

Využitelnost této práce bych viděl v jako představení technologie Internet věcí a jeho využití dnes a v budoucnosti.

Seznam použité literatury a zdrojů

- [1] http://www.ibm.com/ibm/ideasfromibm/cz/smartplanet/opinions/opinion_111708.shtml?ca=neiotcz_smart_planet-20090430&me=w&met=opinions&re=gateway&s_tact=&cm_mmc=-_s-_opinions-gateway-_neiotcz_smart_planet-20090430
- [2] <http://www.kolikje.cz/>
- [3] <http://www.rfid-epc.cz/download/prezen/RFIDWorkingGroup-EPCglobalNet.pdf>
- [4] http://www.gs1cz.org/download/materialy/EPC_rub.pdf
- [5] <http://www.uis.cz/?page=uis-produkty-rfid-identifikace>
- [6] <http://www.bartech.cz/rfid/index.htm>
- [7] http://www.odbornecasopisy.cz/index.php?id_document=39331
- [8] http://www.odbornecasopisy.cz/index.php?id_document=39326
- [9] <http://access.feld.cvut.cz/view.php?cisloclanku=2009020001>
- [10] http://ec.europa.eu/ceskarepublika/press/press_releases/09952_cs.htm
- [11] <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/952&format=HTML&aged=0&language=CS&guiLanguage=en>
- [12] http://cs.wikipedia.org/wiki/IP_adresa#Adresy_v_IPv6
- [13] http://cs.wikipedia.org/wiki/Web_3.0
- [14] <http://www.lupa.cz/clanky/s-mikroformaty-prijde-web-3-0/>
- [15] <http://microformats.cz/>
- [16] <http://eur-lex.europa.eu/>
- [17] <http://www.marketresearch.com/product/display.asp?productid=2529031>
- [18] http://cs.wikipedia.org/wiki/Informa%C4%8Dn%C3%AD_syst%C3%A9m
- [19] <http://www.spsychips.com/>
- [20] <http://www.pooh.cz/pooh/a.asp?a=2010731>
- [21] http://www.stech.cz/index.php?id_document=401155521
- [22] Patrick Plaggenborg, Social RFID - Internet for things, Rotterdam, August 2006

Seznam použitých symbolů a zkratek

- IoT - Internet of Things (internet věcí)
- IT - Information Technology (informační technologie)
- RFID - Radio Frequency Identification (identifikace na rádiové frekvenci)
- EPC - Electronik Product Code
- GPS - Global Positioning System (globální polohový systém)
- Wi-Fi - wireless fidelity
- GPRS - General Packet Radio Service
- EU - Evropská unie
- IS - Information systém (informační systém)

Seznam obrázků

Obrázek 1 Princip funkce RFID.....	4
Obrázek 2 GTIN13 čárový kód	5
Obrázek 3 Schéma EPC kódu	5
Obrázek 4 Schéma logistické firmy (GS1).....	8
Obrázek 5 Čip RFID od firmy Aeroscout	9
Obrázek 6 RFID náramky pro hlídání vězňů	10
Obrázek 7 Mýtná brána v ČR	11
Obrázek 8 Informační systém Pachube.....	17
Obrázek 9 Arduino	18
Obrázek 10 Mir:ror od firmy Violet.....	20
Obrázek 11 Králíček Nabaztag od firmy Violet	20
Obrázek 12 Aplikace WideNoise.....	21
Obrázek 13 Schéma distribuovaného systému	23
Obrázek 14 Systém bezpečnosti dopravy v budoucnosti.....	25
Obrázek 15 Izolovaný systém domu	26
Obrázek 16 Čip určený pro implantaci do ramene	31